

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA

v.

ASIF WILLIAM RAHMAN,

Defendant

Case No. 1:24-CR-249 (PTG)

UNITED STATES SENTENCING MEMORANDUM

When entering on duty, CIA officers swear an oath to support and defend the Constitution of the United States, and to faithfully discharge the duties of their offices. Mr. Rahman deliberately violated that oath and the special trust that the Agency and the U.S. Government placed in him when he disclosed classified information. His actions demonstrate a disregard for the law, for the mission of the CIA, and for U.S. national security interests and the lives of U.S. personnel and our allies.

Michael J. Ellis, Deputy Director of the Central Intelligence Agency

Throughout 2024, the defendant, Asif William Rahman, unlawfully disclosed Top Secret and compartmented national defense information to uncleared people through unsecure systems. In one instance, he disseminated two Top Secret documents about a foreign ally's plans to use kinetic action on an adversary, which became public for the world to see. As an employee with the Central Intelligence Agency (CIA), the defendant swore an oath, received training, and signed multiple non-disclosure agreements to protect the nation's most classified secrets. He was entrusted to keep this country, and its allies, safe. But he abused that trust, risking, by definition, *exceptionally grave damage* to the national security of the United States. And Rahman knew what he had done was illegal, so he worked to avoid detection: In the days and weeks following his conduct, he deleted information and destroyed devices. Normally, as further supported by the details in the government's classified supplemental memorandum, the defendant's conduct would

warrant an upward variance from the potentially applicable Guidelines range (58-71 months)¹ to a statutory maximum sentence of 120 months' imprisonment.

The defendant, however, cooperated and confessed swiftly. Within less than a month of the defendant's criminal conduct going public, the FBI arrested him overseas; within three months of his conduct, he pled guilty. His post-arrest decisions helped to solidify a certainty and celerity that people who engage in such unlawful disclosures will be prosecuted and brought to justice. That general deterrence matters, especially considering the volume of people across the world with access to the nation's most sensitive information related to national security.

This case presents a number of factors for the Court to consider in imposing a just sentence: Rahman is a defendant whose egregious conduct posed a significant national security threat, but he confessed and cooperated quickly. The applicable Guidelines range fails to capture the full extent of the defendant's acts and potential harm, but the Court should also balance that need with defendant's post-arrest conduct and its impact on deterrence. The government has endeavored to engage in that balancing, presenting its efforts in this memorandum and the government's classified supplemental memorandum. Attached to this memorandum is an unclassified letter the government received from the Deputy Director of the CIA, and attached to the classified memorandum are classified intelligence community declarations. Ultimately, the government submits that a sentence of 108 months' imprisonment is a sufficient, but not greater than necessary, sentence to comply with the purposes of sentencing set forth in 18 U.S.C. § 3553(a).

¹ As further detailed below, the government has determined the defendant's cooperation constituted "substantial assistance" under Guidelines § 5K1.1, and hereby moves to depart downward by one offense level, bringing his total offense level from the agreed-upon 26 to 25. Should the Court grant the government's motion, the defendant's applicable Guidelines range would be 58-71 months.

PROCEDURAL BACKGROUND

On November 7, 2024, a grand jury sitting in the Eastern District of Virginia returned an indictment charging Asif William Rahman, who was then employed as a Central Intelligence Agency analyst, with two counts of willful retention and transmission of national defense information (NDI), in violation of 18 U.S.C. § 793(e). Presentence Investigation Report (PSR) at ¶ 1. On November 12, 2024, the Federal Bureau of Investigation (FBI) arrested the defendant overseas. *Id.* On January 17, 2025, the defendant appeared before this Court and entered a plea of guilty to Counts One and Two of the Indictment. *Id.* at ¶ 2. Sentencing is currently scheduled for May 13, 2025. *Id.*

FACTUAL BACKGROUND

The Defendant's CIA Employment and Access to Classified Information

The defendant began working for the CIA in 2016. PSR at ¶ 22. As required for his employment, the defendant possessed a TS//SCI (Top Secret//Sensitive Compartmented Information) United States government security clearance and had access to NDI classified up to the TS//SCI level. *Id.* By law, national security information classified as 'TOP SECRET' was information owned by, produced by, produced for, and under the control of the United States government, the unauthorized disclosure of which, by definition, reasonably could be expected to cause exceptionally grave damage to the national security of the United States. *Id.* at ¶ 23. Indeed, the defendant's access to SCI information meant he was entrusted with handling information further protected through compartments to protect particularly sensitive intelligence sources and methods. *Id.* at ¶ 25. Authorized access to SCI required an appropriate security clearance, nondisclosure agreement, need to know, and additional SCI permissions, and storage of SCI was only authorized within an approved Sensitive Compartmented Information Facility (SCIF). *Id.*

Notably, the defendant understood all of these protocols surrounding classified information and agreed to abide by them to protect and defend the country. In connection with his employment, the defendant signed a Classified Information Nondisclosure Agreement and multiple SCI Nondisclosure Agreements, most recently on January 5, 2023. *Id.* at ¶ 27. Beyond warning the defendant that unauthorized disclosure of classified information was punishable under United States law, the defendant's signed agreement noted:

I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government or Agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department of Agency or a contactor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be, or related to or derived from SCI, is considered by such department or Agency to be SCI. I further understand that I am obligated by law and regulation not to disclose any classified information or material in an authorized fashion.

Id.

The Defendant's Multiple Unlawful Transmissions of Classified NDI

Throughout 2024, the defendant violated this agreement, disclosing some of the most sensitive intelligence information in the United States government.²

² In light of the classified nature of the materials and information underlying the defendant's unlawful disclosures, the government's classified supplemental memorandum provides additional details of the defendant's actions.

Spring 2024

In the spring of 2024, for example, the defendant accessed and printed from his workstation approximately five documents classified at the Secret and Top Secret levels. *Id.* at ¶ 28. The defendant concealed the materials in his backpack and transported them to his house. *Id.* There, he reproduced the documents and altered the images to conceal their source and his criminal activity. *Id.* Before disclosing the images of classified documents, he communicated Top Secret information he learned during his employment to multiple people he knew were not entitled to receive it. *Id.* He then transmitted the images of Secret and Top Secret classified documents to multiple other people he knew were not entitled to receive them. *Id.* After his unlawful disclosures, the defendant deleted his activity from a variety of electronic devices and returned to his workstation with the classified documents where he shredded them.

Fall 2024

The defendant would follow this pattern of behavior throughout the rest of the year. In the fall, the defendant accessed and printed over ten documents classified at the Top Secret level. *Id.* at ¶ 29. He again put those documents in a backpack, took them to his house, and made images of the documents that he altered to conceal their source and his criminal activity. *Id.* Before disclosing the images of the documents, the defendant communicated Top Secret/SCI information—including information subject to further compartmentation—he learned during his employment to multiple people he knew were not entitled to receive that information. *Id.* He then transmitted the images of the Top Secret documents to multiple people he knew were not entitled to receive them. *Id.* Like in the spring, the defendant then deleted activity and information from his electronic devices and returned to his workstation with the classified documents where he shredded them. *Id.*

October 17-18, 2024

By October 2024, the defendant had made a practice of disclosing highly classified information to others outside of the United States government. A pattern he followed until he was arrested.

On October 17, 2024, the defendant accessed and printed approximately two documents regarding a United States' foreign ally and its planned kinetic actions against a foreign adversary ("Documents One and Two"). *Id.* at ¶ 30. Documents One and Two were classified at the Top Secret level and contained NDI. *Id.* A United States government agency had only generated these documents a day earlier, on October 16, 2024. *Id.* Yet, within twenty-four hours, the defendant was walking out of his workstation and to his house with them in his backpack. *Id.* At his residence, the defendant photographed the documents and transferred those images to a computer program that allowed him to edit the images in an attempt to conceal their source and delete his criminal activity afterward. *Id.* Before disclosing the documents, the defendant communicated Top Secret NDI he learned during his employment to multiple people he knew were not entitled to receive them. *Id.* Then he sent the images of Top Secret Document One and Top Secret Document Two, both of contained NDI, to multiple people he knew were not entitled to receive them. *Id.*

By October 18, 2024, the defendant received written confirmation from one of the people not entitled to receive classified NDI that they had received the information and further distributed Document One and Document Two to others. *Id.* at ¶ 31. Because of the defendant, those documents would spread across the world in a matter of minutes. Documents One and Two appeared publicly on multiple social media platforms, complete with the classification markings.

Id. at ¶ 32. On one of the social media platforms, the user that posted the documents added the following caption:

EXCLUSIVE: An informed source within the U.S. intelligence community has shared with us an extremely sensitive “top secret” U.S. intelligence document from the [U.S. government agency], dated October 15-16, detailing [foreign ally] preparations for an extensive strike inside [foreign adversary] . . . This classified report originates from the [U.S. government agency], part of the U.S. Department of Defense.

Id.

Afterward, the defendant deleted his activity from electronic devices and returned to his workstation with Documents One and Two where he shredded them. *Id.* at ¶ 33.

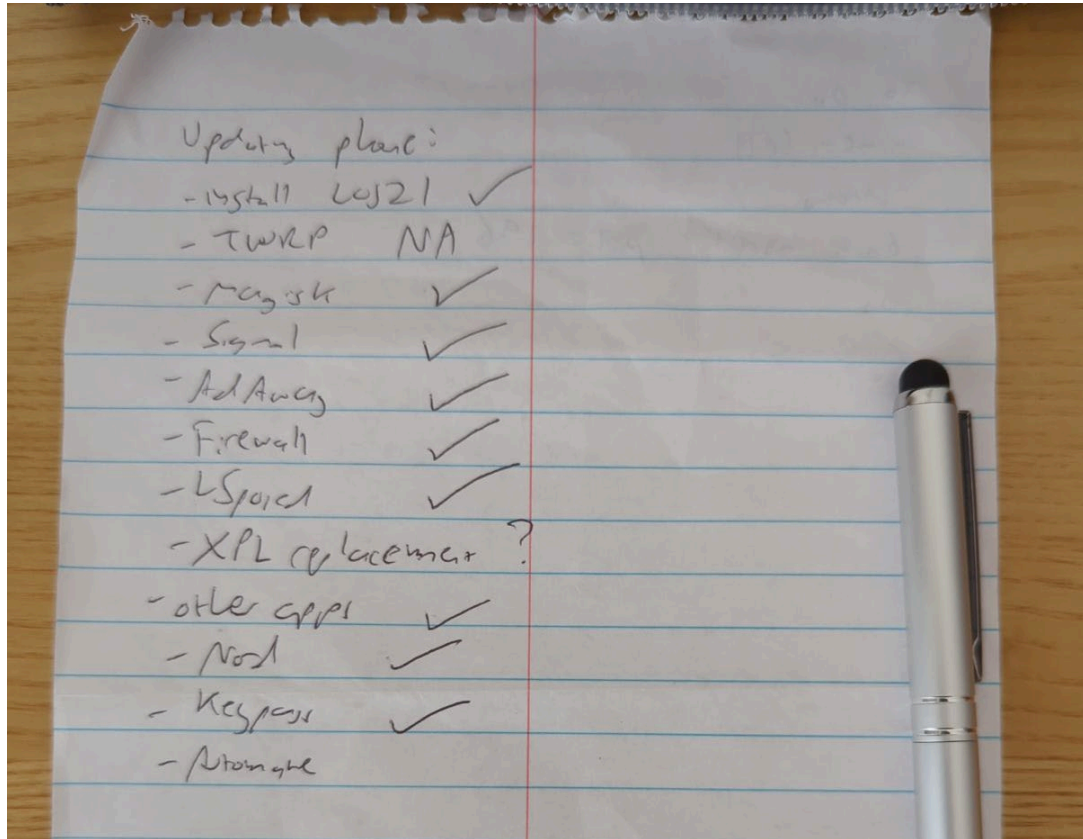
Late Fall 2024

Despite the virality of the defendant’s criminal conduct and the highly publicized nature of the Top Secret classified information he disclosed, he continued. During late Fall 2024, the defendant used secure platforms to communicate Top Secret information he learned during his employment to multiple people he knew were not entitled to receive them. *Id.* at ¶ 34. And, throughout his criminal conduct, the defendant maintained and updated certain notes related to Top Secret information on multiple pieces of paper he kept on his person. *Id.* at ¶ 35. In them, the defendant cryptically documented some of the Top Secret information via sequences of letters and numbers intending, in part, to later transmit that information to people he knew were not entitled to receive classified information. *Id.* Notably, some of the pages discovered on the defendant’s person at the time of arrest included cryptic strings of letters and numbers written under the header, “To Do;,” indicating the defendant’s intent to continue his crimes.

The Defendant's Efforts to Conceal His Criminal Conduct

The defendant took a number of steps to conceal his unlawful disclosures:

First, the defendant's desk at his home included a handwritten list of applications and software outside of any government-suggested platforms—all intended to fortify Android electronic devices against interception and discovery. That checklist is depicted below:



The applications included not only common encrypted messaging platforms, but also more unusual software used to customize and modify mobile devices including by “root access” to a phone’s operating system. Based on an extraction of a device found at the defendant’s residence, he had downloaded and installed nearly all of his listed applications that would allow him to root his device and fortify well it beyond standard, factory protections. And, at the time of his eventual arrest, the defendant possessed on his person and at his residence a number of electronic devices,

including three total phones, multiple laptops, and multiple large-capacity external hard drives—nearly all powered off and highly encrypted.

Second, the defendant deleted Top Secret materials from his workstation. From in or around early 2019, through in or around fall 2020, the defendant accessed and downloaded thousands of highly classified intelligence reports as part of his employment. *Id.* at ¶ 37. Many of those reports required highly compartmented access. *Id.* The defendant was debriefed, or “read out,” from those reporting compartments in or around fall 2020. *Id.* By October 21, 2024, however, the defendant still maintained some of these records in his email and personal folder on his Top Secret workstation. *Id.* So, on October 21, 2024, after his disclosures of Documents One and Two appeared across the internet and were on nearly every major news site across the world,³

³ CNN (<https://www.cnn.com/2024/10/19/politics/us-israel-iran-intelligence-documents>); PBS (<https://www.pbs.org/newshour/world/u-s-officials-investigate-leak-of-classified-documents-that-describe-israels-attack-plans>); Reuters (<https://www.reuters.com/world/us/investigation-underway-into-leak-us-intelligence-israel-iran-houses-johnson-says-2024-10-20/>); BBC (<https://www.bbc.com/news/articles/cz6w6p8x7p8o>); NPR (<https://www.npr.org/2024/10/20/nx-s1-5158977/leaked-documents-describe-possible-israeli-strike-on-iran>); The Guardian (<https://www.theguardian.com/us-news/2024/oct/20/leaked-documents-allege-israel-plans-attack-iran>); CBS News (<https://www.cbsnews.com/news/us-investigating-israel-attack-plans-iran-unauthorized-release-classified-documents/>); NBC News (<https://www.nbcnews.com/news/us-investigating-apparent-leak-top-secret-us-documents-israel-rcna176286>); The New York Times (<https://www.nytimes.com/2024/10/19/us/politics/us-intelligence-israel-iran.html>); The Washington Post (<https://www.washingtonpost.com/national-security/2024/10/22/israel-iran-intel-leak-fbi/>); Al Jazeera (<https://www.aljazeera.com/news/2024/10/21/biden-concerned-about-release-of-files-on-israels-plans-to-strike-iran>); Yahoo! News (https://www.yahoo.com/news/purported-leaked-us-intelligence-docs-221200587.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLnNvbS8&guce_referrer_sig=AQAAAHLLHMGpaxDYucGGxzz3L_iBlmtsg1HlCwR52bJMd91SFdI_HHkxEhe8I1fwr_WFhdYp8AeY6iuBr4dL7k_b-iMyk_f_gaTqkvvR8KERLUSq-hf-292f4xyQRiHnVga_rpttHhjOtqBmoq25vUrmBvDtWhnpWAE_LAL-bsngTI52); ABC News (<https://abcnews.go.com/US/purported-leaked-us-intelligence-docs-show-israels-plans/story?id=114958696>)

the defendant deleted those files. *Id.* In fact, between October 23, 2024, and October 31, 2024, the defendant deleted approximately 1.5 gigabytes of data from his email and personal folder on a Top Secret workstation, in part to conceal his access to the compartmented information. *Id.*

Third, the defendant deleted and edited certain journal entries and written work product on his personal electronic devices to conceal his personal opinions on United States policy. He took these steps, in part, to construct a false, innocuous narrative regarding his deletion of certain records on his personal devices and CIA workstation. *Id.* at ¶ 38.

Fourth, after October 17, 2024, the defendant destroyed multiple electronic devices, including his personal Galaxy Samsung A3 mobile device and an internet router he used to transmit the classified information and photographs of classified documents. *Id.* at ¶ 39. Then he discarded the destroyed devices in public trash receptacles through his neighborhood overseas to thwart potential investigations into him and his unlawful conduct. *Id.*

APPLICABLE SENTENCING GUIDELINES

The advisory guidelines range, as calculated pursuant to the United States Sentencing Guidelines is not binding upon the Court and instead constitutes a “starting point and initial benchmark” in the sentencing analysis. *Gall v. United States*, 552 U.S. 38, 49-50 (2007). Nonetheless, “a court of appeals may apply a presumption of reasonableness to a sentence imposed by a district court within a properly calculated guideline range” Guidelines Manual, published November 1, 2024, at 14 (citing *Rita v. United States*, 551 U.S. 338 (2007)). After ensuring that the advisory guideline range is properly calculated, the Court must consider whether a sentence within that range serves the factors and purposes set forth in 18 U.S.C. § 3553(a). *See United States v. Moreland*, 437 F.3d 424, 432 (4th Cir. 2006). If it does not, the Court must determine whether grounds for a departure exist under the guidelines or pertinent case law and apply them,

as appropriate. *Id.*; see also *United States v. Tucker*, 473 F.3d 556, 560-61 (4th Cir. 2007) (consider departure ground before imposing variance). If, following that analysis, the Court still deems a sentence within the advisory guidelines range to be inadequate, the Court may further vary, above or below, that advisory range until it reaches a sentence that best serves the statutory sentencing factors and purposes. See *Moreland*, 437 F.3d at 432. Finally, the Court must state its reasons for imposing such a sentence, taking care to explain the reasons for any departure or variance. *Id.*; see also 18 U.S.C. § 3553(c)(2).

The government agrees with the Guidelines calculation in the PSR, which tracks with the calculation of the Guidelines set forth in the Plea Agreement. ECF 57. The counts in the Indictment group under Guidelines § 3D1.2(a), because the United States Government is the victim and the defendant's actions were part of the same act of willfully transmitting information related to the national defense which he had reason to believe could be used to the injury of the United States and to the advantage of a foreign nation. See PSR ¶ 49. Therefore, the count with the highest offense level in the Indictment should be used to calculate the Guidelines. Guidelines § 3D1.3(a). Here, that is either Count One or Count Two in the Indictment, which both charged the defendant with the willful retention and transmission of National Defense Information, in violation of 18 U.S.C. § 793(e). See PSR ¶¶ 50-59.

The Government agrees with the PSR that Guidelines § 2M3.3 applies to a conviction of 18 U.S.C. § 793(e). *Id.* at ¶ 50. As to the defendant's unlawful transmissions underlying the charges, the defendant used his position of trust as an analyst with the CIA and accessed and printed two documents regarding the United States' foreign ally and its planned kinetic actions against a foreign adversary. He then transported those documents outside of his place of employment and to his residence, where he transmitted images of the documents to multiple

individuals he knew were not entitled to receive them. These documents were classified at the Top Secret level and contained National Defense Information. Therefore, the base offense level is 29. *Id.* ¶ 50.

The Government also agrees with the two-level upward adjustment the PSR recommends and the parties agreed to in the plea agreement regarding the defendant's abuse of his position of trust. As a CIA intelligence analyst with a Top Secret/SCI security clearance, the defendant abused his position of public trust in a manner that significantly facilitated the commission of his crimes. He had access to the information that he unlawfully transmitted to others because of his role in the U.S. Intelligence Community and his security clearance. Therefore, Guidelines § 3B1.3 applies and the offense level should be increased by two more levels to 31. *See* PSR ¶ 53; *see also United States v. Barringer*, 25 F.4th 239, 253-58 (4th Cir. 2022) (upholding application of § 3B1, stating in part that courts consider factors "from the victim's point of view," including "whether the defendant had special duties or special access to information not available to other employees") (citation omitted); *United States v. Ford*, 288 F. App'x 54, 60-61 (4th Cir. 2008) (per curiam) (upholding application of § 3B1.3 to TS/SCI clearance holder convicted of violating 18 U.S.C. § 793, stating the defendant "held a top secret security clearance as an employee of the National Security Agency and he was able to remove classified documents from his office without detection by his supervisors. [The defendant's] actions exposed classified information to discovery by a person without a security clearance and created a potential for serious harm to our nation's security."); *United States v. Pitts*, 176 F.3d 239, 246 (4th Cir. 1999) ("It is certainly also important to inquire into the level of harm occasioned by the breach of trust."); *United States v. Mallory*, Case No. 1:17-cr-154, Dkt. 280, at 16 (E.D. Va. July 30, 2019) (Ellis, J.) ("He only retained the

information because of the position of trust that he held at the time that he was employed by the agency.”).

Lastly, the Government agrees with the PSR recommendations regarding reductions to the applicable offense level. The defendant should receive a two-level downward adjustment for acceptance of responsibility under Guidelines §§ 3E1.1(a). PSR ¶¶ 56-57. Based on the defendant’s assistance “in the investigation [and] prosecution of his own misconduct by timely notifying authorities of his intention to enter a plea of guilty,” the government hereby moves this Court for an additional one level decrease, totaling to three levels for acceptance of responsibility. *See* Guidelines § 3E1.1(b). And the defendant appears to meet the criteria under Guidelines § 4C1.1(a), warranting an additional two-level downward adjustment.

In sum, the defendant’s total Guidelines offense level is 26, *see* PSR ¶ at 59, and his criminal history category is I, *see id.* at ¶ 62. Before any consideration of the defendant’s cooperation, the defendant’s applicable Guidelines range is 63 to 78 months. *See id.* at Part D, ¶¶ 90-91.

Based on the government’s assessment that the defendant’s cooperation amounted to “substantial assistance,” the government moves for a one-level downward departure under Guidelines § 5K1.1. The defendant appears to have provided truthful information related to others. As noted in further detail in the government’s classified supplemental memorandum, however, while the defendant’s cooperation qualified as substantial, it has not led, and likely will not lead, to the prosecution of others. And the remainder of defendant’s cooperation largely amounted to corroboration of information the government previously knew. While this cooperation can still be substantial in national security cases, it warrants a smaller downward departure than in cases where the government learns largely new information that leads to additional prosecutions or disruptions.

As such, a one-level downward departure is warranted, and the revised applicable Guidelines range should be 58-71 months' imprisonment.

ARGUMENT

Considering the full scope of the defendant's conduct, detailed further in the government's classified supplemental memorandum, it is clear the applicable Guidelines range of 58-71 months is woefully inadequate, warranting a significant upward variance. Indeed, that range would be applicable had the defendant willfully transmitted just *one single* document with Top Secret National Defense Information to another without clearance. Simply put: the applicable Guidelines range does not account for the quantity and quality of Top Secret, compartmented information the defendant unlawfully disclosed throughout 2024 and the potential danger he created to national security. That said, the defendant's timely confession and plea was extraordinary, helping to send a deterrent message to would-be criminals considering disclosing classified NDI. Balancing these considerations, a sentence of 108 months' imprisonment is appropriate.

In addition to the applicable Guidelines range, the factors for the district court to consider at sentencing include: (1) the nature and circumstances of the offense; (2) the history and characteristics of the defendant; (3) the important need for the sentence to reflect the seriousness of the crime and respect for the law; the (4) the need to deter future criminal conduct; and (5) the need to avoid unwarranted sentencing disparities. 18 U.S.C. § 3553(a).

1. Nature and Circumstances of the Offense

The nature of the defendant's conduct is extraordinarily serious. Section 793(e) prohibits a range of conduct that varies in severity. On one end of the spectrum, the statute prohibits simply unlawfully retaining certain information; on the other, the statute prohibits transmitting that information to others. The latter warrants a more significant punishment in light of the increased

risk it presents to the nation's security, as seen in this case. Indeed, the defendant's violations of the Espionage Act consisted of not only removing and retaining classified NDI but also repeatedly, and purposefully, transmitting that classified information to others. Two of his unlawful disclosures remain to this day publicly available to anyone with an internet connection, including the nation's adversaries, to digest. More troublingly, it is impossible for the government to fully know the extent to which the defendant's many other disclosures have spread across foreign adversaries' networks. This conduct is far more significant than retention alone. While unauthorized retention results in an unacceptable risk that national defense information will be released to strangers and adversaries, transmission offenses like the defendant's *ensure* that it will. *See United States v. Ford*, 288 F. App'x 54, 61 (4th Cir. 2008) (affirming sentencing where court recognized that the active transmission of classified national defense information should be punished more harshly than retention).

When our nation's secrets are published, especially online, those secrets are made available to all of our adversaries. In fact, a foreign military officer from Russia confirmed as much when he wrote "I was amazed—and Moscow was very appreciative—at how many times I found very sensitive information in American newspapers. In my view, Americans tend to care more about scooping their competition than about national security, which made my job easier." Stanislav Lunev, *Through the Eyes of the Enemy* 135 (Regnery Publishing, Inc.) (1998).

The vital need for the government to collect intelligence and safeguard its secrets to protect our people and defeat our adversaries dates as far back as General George Washington and his efforts in the Revolutionary War. On July 26, 1777, General Washington wrote to Colonel Elias Dayton, who headed Washington's spy ring against the British Army on Staten Island, in part stating:

The reason of my being thus particular in describing Lord Stirlings Rout, is, Because I wish you to take every possible pains in your power, by sending trusty persons to Staten Island in whom you can confide to obtain intelligence of the Enemy's situation & numbers. . . . The necessity of procuring good Intelligence is apparent & need not be further urged—All that remains for me to add, is, that you keep the whole matter as secret as possible. For upon Secrecy, Success depends in most Enterprizes of the kind, and for want of it, they are generally defeated, however well planned & promising a favourable issue.⁴

“From George Washington to Colonel Elias Dayton, 26 July 1777,” *The Papers of George Washington*, Revolutionary War Series, vol. 10, *11 June 1777–18 August 1777*, ed. Frank E. Grizzard, Jr. Charlottesville: University Press of Virginia, 2000, pp. 425–426.

The complexity of the intelligence has grown over time, but the need to preserve its secrecy remains. If anything, the import of preserving our nation's most sensitive intelligence to secure national security has only grown. Former CIA Director George Tenet once confirmed the risk created by broad dissemination of our nation's secrets:

I just need to reinforce that when you throw this [classified] information out, it often appears innocuous to someone who's leaking information. That's not the prism to look at it in. It's the adversary's counterintelligence. And his ability to put together the pieces of the puzzle that put at risk your human operations, your technical operations, your analytical products, and jeopardizes investment that we've made to protect the American people.

Hearing before the Senate Select Committee on Intelligence: Current and Projected National Security Threats to the United States, S. Hrg. 106–580, p. 158 (February 2, 2000).⁵

This sentiment was echoed a few years later by a subsequent CIA Director, Porter J. Goss, who also underscored the damage caused by leaks of classified information:

[F]or all the successes we have had and the advances we have made, serious and unnecessary damage has been caused by media leaks. Unauthorized disclosure of

⁴ Available at <https://founders.archives.gov/documents/Washington/03-10-02-0415>.

⁵ Available at <https://www.govinfo.gov/content/pkg/CHRG-107shrg82338/html/CHRG-107shrg82338.htm>.

classified information threatens the survivability of the sources and methods that we depend upon. We have lost opportunity, if not capability, because of irresponsible leaks and this has made it easier for our enemies.

Hearing Before the Senate Select Committee on Intelligence: Current and Projected National Security Threats to the United States, S. Hrg. 109-363, p. 5 (March 17, 2005).⁶

The defendant dismissed this history, discarded his training, and jeopardized national security throughout 2024. The applicable Guidelines range falls far short of capturing the volume and magnitude of the defendant's full conduct. As laid out in the Government's classified supplemental memorandum and the associated classified declarations, the government cannot overstate the potential harm the defendant's actions presented. *See, e.g., United States v. Morison*, 844 F.2d 1057, 1071 (4th Cir.1988) (explaining the government need not show there was actual harm to the national security from the defendant's unauthorized disclosure; rather, the government must show there was the *potential* for harm to the national security).

The defendant's conduct was purposeful and, shockingly, ongoing. He systematically and methodically stole classified national defense information and provided it to others outside of the government—even after one of his disclosures exploded across the internet and should have caused him to stop. His criminal conduct was not the result of a momentary lapse of judgment; rather, for nearly a year, the defendant spent time at work printing and preparing to disseminate Top Secret information and documents. And he spent time at home cautiously manipulating images of the classified NDI to obscure their source and conceal his involvement, later shredding the documents and deleting his digital trail. The defendant did all this knowing full well that it was illegal, that it was harmful to the United States, and that it was reasonably foreseeable the information could be

⁶ Available at <https://www.govinfo.gov/content/pkg/CHRG-109shrg27088/html/CHRG-109shrg27088.htm>.

used to benefit foreign adversaries.

But the defendant's deception did not stop with his disclosures. Once the defendant knew he would be caught, he took steps to conceal his disclosures by deleting evidence and destroying devices. On October 22, 2024, news outlets, including the Washington Post, quoted then-FBI Director Wray: "The FBI is investigating the alleged leak of classified documents and working closely with our partners in the Department of Defense and Intelligence Community."⁷ And, by October 24, 2024, CNN quoted an anonymous United States official among others in reporting that the "FBI is zeroing in on a US government office where it believes the leaked US intelligence documents on Israel's preparations for a possible attack were printed."⁸ That same week, the defendant took a number of obstructive steps to conceal his criminal acts, engaging in a deletion campaign of 1.5 gigabytes of data on his Top Secret workstation, deleting and cultivating his writings on his personal electronic devices, and destroying certain electronic devices he used to commit his crimes. Worse, as detailed in the government's classified supplemental memorandum, the defendant engaged in *additional* classified disclosures after these news reports in an attempt to conceal his conduct and prevent the government from identifying and arresting him. Notwithstanding his efforts, the defendant could not delete all evidence of his unlawful disclosures of classified information, especially as images of classified information foreseeably became widely distributed around the globe.

⁷ Available at <https://www.washingtonpost.com/national-security/2024/10/22/israel-iran-intel-leak-fbi/>.

⁸ Available at <https://www.cnn.com/2024/10/24/politics/fbi-zeroing-leaked-us-intel-documents-printed/index.html>.

2. Defendant's History and Characteristics

The history and characteristics of the defendant also favor a significant sentence. The defendant is a 34-year-old former CIA analyst. PSR at 3. He worked in the intelligence community for nearly eight years before committing these crimes. He was a sophisticated intelligence professional, who had received extensive training in the proper handling of classified information and signed multiple agreements to do so. *Id.* at ¶ 27. Based on his training and work as an intelligence analyst, the defendant *knew* the potential harm to the national security that could result from the unauthorized disclosure of classified NDI. *Id.* Despite this understanding, the defendant disclosed highly classified information that could be damaging to the United States and used to the advantage of this country's adversaries.

By all accounts, the defendant had the kind of upbringing many defendants that appear before this Court could only dream of. Surrounded by a robust support system led by a two-parent household, the defendant reportedly grew up in a safe, upper-middle-class neighborhood where his basic needs were always met. PSR at ¶ 68. He experienced no issues of domestic violence, substance abuse, or mental health and has never experienced sexual assault. *Id.* When he left his family for school, the defendant had the opportunity to attend some of the best schools in the country—including Yale University for his bachelor's degree and the University of Chicago for his Master of Business Administration. *Id.* at ¶¶ 77-78. And during that time and after, the defendant secured lucrative positions at various financial firms. *Id.* at ¶¶ 81-82. According to the PSR, the defendant and his spouse experienced certain personal life experiences leading up to the time of his criminal conduct throughout 2024. While these circumstances are certainly tragic, there is no indication that they directly led to the defendant's choice to willfully and blatantly violate the Espionage Act. Indeed, the CIA was an opportunity for the defendant to work hard and

provide a stable life for his family. Despite his privileged upbringing and prestigious opportunities in the academic, financial, and intelligence worlds, the defendant put his country in danger. That is a history that warrants not leniency, but significant punishment.

3. Just Punishment, Seriousness of the Offense, and Respect for the Law

An above-guidelines sentence is necessary to provide just punishment and appropriately reflect the seriousness of the offense. As the Supreme Court has noted, “[i]t is ‘obvious and unarguable’ that no governmental interest is more compelling than the security of the Nation.” *Haig v. Agee*, 453 U.S. 280, 307 (1981) (citations omitted). And “[e]spionage is one of this nation’s most serious offenses.” *United States v. Whitworth*, 856 F.2d 1268, 1289 (9th Cir. 1988). It is antithetical to American public service and often puts lives at risk. It also can cost the U.S. government greatly, forcing it to adjust military planning, operations, and tactics to account for compromises in informational security.

Even in an unclassified setting and at a general level of detail, the seriousness of the offense is abundantly clear. As the defendant agreed in his Statement of Facts, the defendant repeatedly disclosed Top Secret and, at times, further compartmented information and documents that he stole from his workstation and transported to his house. Just one example of those documents highlights how serious the information is to the United States and its allies (and, troublingly, our adversaries): the documents underlying Counts One and Two were Top Secret documents that discussed “a United States foreign ally and its planned kinetic actions against a foreign adversary.” ECF 58 at 4. The harm from disclosing that the U.S. had intelligence on a foreign ally’s planned actions against a foreign adversary should be apparent. When combined with the full scope of the defendant’s conduct, that harm multiplies exponentially. The Government is limited in what it can say in an unclassified setting regarding the seriousness of the defendant’s conduct throughout

2024. But, attached to the government’s unclassified sentencing memorandum is a letter from CIA Deputy Director Michael Ellis, in which he explains the gravity of the defendant’s conduct: “At an unclassified level . . . Mr. Rahman’s reckless and unlawful actions jeopardized intelligence sources and methods, undermined U.S. intelligence-sharing partnerships, and compromised information regarding sensitive intelligence targets of interest.” Exhibit 1, CIA Deputy Director Michael J. Ellis Letter. The Government’s classified supplemental memorandum and the classified declarations and associated attachments from multiple intelligence agencies set out in more detail the catastrophic harms that could have occurred because of the defendant’s actions.

Separately, the defendant’s conduct during his employment with the CIA highlights just how little respect he had for the law and his signed agreements with the government to protect its information. When the defendant joined the CIA, he was granted a security clearance, entrusted to protect intelligence that contributed to the safety and security of the nation. Through his actions, however, the defendant allowed the United States’s most significant adversaries to have access to some of the country’s most closely guarded intelligence. And, as detailed above, the defendant gained access through his employment to thousands of classified documents about a particular region in the world throughout 2020 and, by 2021, was removed from that access and “read out” of the program. By law, he no longer was authorized to access those materials. But, within days of his October 17 transmission of highly sensitive NDI, he not only had retained some of those materials on his personal workstation, but also rapidly began deleting gigabytes of them. Disclosing and deleting classified materials illustrates his profound lack of respect for the law.

4. The Need for Adequate Deterrence and Protecting the Public

A 108-month sentence will provide adequate deterrence as to the defendant and provide a reasonable amount of protection from future criminal activity. But the Court is also obligated to

consider the issue of general deterrence, which is particularly important as applied to convictions under the Espionage Act. Here again, a sentence within the guidelines is insufficient in light of the magnitude of the defendant's actions. Trust is essential to the effective functioning of the Intelligence Community. There must be significant consequences when that trust is breached, especially when it is breached in the defendant's manner. This is particularly true in the era of social media where the government's secrets can be shared around the world with the click of a mouse. The Court's sentence must send a message that reinforces the importance of faithfully honoring promises to safeguard the secrets of our nation.

That said, the defendant's swift acceptance of responsibility and plea play a vital role in the government's attempt to accomplish maximum general deterrence in this case. "The classical theory of deterrence developed from the work of three modern philosophers: Thomas Hobbes (1651), Cesare Beccaria (1764), and Jeremy Bentham (1789). They believed that if punishment is *severe, certain, and swift*, a rational individual will weigh potential gains and losses before engaging in illegal activity and will be discouraged from breaking the law if the loss is greater than the gain." "Classical deterrence theory revisited: An empirical analysis of Police Force Areas in England and Wales," *European Journal of Criminology*, 20(5), 1663-1680, Abramovaite, J., Bandyopadhyay, S., Bhattacharya, S., & Cowen, N. (2022) (emphasis added).⁹ These three concepts—severity, certainty, and celerity (or "swiftness")—are fundamental to the concept of deterrence. *Id.*

Certainty. "Certainty of punishment has been the most explored area [of analyzing crime rates] and there is now a relatively strong consensus that increasing the likelihood of apprehension

⁹ Available at <https://journals.sagepub.com/doi/10.1177/14773708211072415>.

reduces crime based on most empirical studies.” *Id.* (citing studies). Here, part of the deterrent message stems from the government’s success in identifying and arresting the right subject despite his efforts to prevent that identification. The defendant concealed classified documents in his backpack, digitally altered them at his house to conceal their source, deleted his digital activity, and shredded the documents when he returned to work. As noted above, he engaged in sophisticated encryption efforts on his personal devices and, after his criminal conduct became public, he deleted information and destroyed devices. Despite doing this from across the world, the government identified him and arrested him. The message of certainty, and its impact on deterrence, in this case is profound: If you disclose the nation’s most-guarded secrets related to national security and defense, the government will find you, wherever you are in the world, and seek justice.

Celerity (Swiftness). As to celerity, or how swift the defendant will face justice for his conduct, the defendant’s conduct became public on or about October 18, 2024, when his unlawful disclosures of Top Secret NDI went viral across the internet. By November 7, 2024—twenty days after his crime went overt—the government had identified the defendant as the subject responsible, located him overseas, and secured an indictment from a federal grand jury sitting in the Eastern District of Virginia. And, by November 12, 2024, the FBI executed the arrest warrant and placed the defendant in custody, transporting him to the District of Guam and, eventually, the Eastern District of Virginia.

The defendant’s actions were extraordinary too. His swift confession and plea was notable, and the Court should consider it significantly in determining a just sentence. Related to the certainty of punishment, the speed with which the government arrested the defendant and with which the defendant confessed and pled guilty in open Court powerfully compounds the

government's message of deterrence to the world of those considering disclosing classified NDI. Indeed, the defendant's plea punctuated the government's message of deterrence by announcing that not only will the government find you, but it will build a case strong enough to lead to convictions in a timely manner. The impact of the defendant's decision to plead so quickly is obvious just by reading what the Department of Justice's leadership focused on in their press release quotes on the day of his plea:¹⁰

- **Matthew Olsen, then-Assistant Attorney General of National Security:** “Mr. Rahman betrayed the trust of the American people by unlawfully sharing classified national defense information he swore an oath to protect. Today’s guilty plea demonstrates that the Justice Department will spare no effort to *swiftly* find and aggressively prosecute those who harm the United States by illegally disclosing our national security secrets.” (emphasis added);
- **Jessica Aber, then-United States Attorney for the Eastern District of Virginia:** “Asif Rahman is pleading guilty in federal court three *months to the day* that he disclosed top secret American documents in violation of his oath, his responsibility, and the law. This District, in partnership with federal law enforcement and the intelligence community, exemplified dedication, skill, and *speed* to bring him to justice *expeditiously*. Mr. Rahman’s actions placed lives at risk, undermined U.S. foreign relations, and compromised our ability to collect vital intelligence in the future.” (emphasis added);
- **David Sundberg, then-Assistant Director of the FBI Washington Field Office:** “Today’s plea demonstrates the FBI’s resolve to deploy the necessary tools and authorities

¹⁰ Available at <https://www.justice.gov/archives/opa/pr/former-cia-analyst-pleads-guilty-transmitting-top-secret-national-defense-information>.

to identify, locate, and bring to justice a government clearance holder who violated the oath he took to support and defend the U.S. Constitution. This is a good reminder to all clearance holders that the FBI and our Intelligence Community partners will spare no resource to *immediately* find and hold accountable those who violate the law and disclose classified information without authorization, *no matter where in the world they are located.*” (emphasis added).

Beyond the standard resources the government saved in resolving the case short of trial, the defendant’s rapid decision to accept responsibility and publicly plead guilty has helped the government spread the message of general deterrence far and wide. Also worth considering, as described in more detail in the classified supplemental memorandum, is that the defendant’s benefit from his swift acceptance of responsibility has already actualized in some ways: by pleading guilty, the government’s investigation halted, thereby ending the case before the government may have developed additional evidence to impose more significant charges with more severe Guidelines calculations here.

Severity. This case warrants a significant punishment to deter those with access to the nation’s secrets from revealing them to our adversaries. In just one example of the many documents and wealth of information the defendant transmitted, the October 17 documents comprised of Top Secret materials related to the active plans, preparation, and capabilities of a foreign ally to attack a foreign adversary. *See* PSR at ¶ 10; ECF 25-1 (“NGA Declaration in Aid of Detention”), ECF 25-2 (“CIA Declaration in Aid of Detention”). This is not information related to a single individual or even a single localized community; this information pertained to entire nation states and their armed forces. It is hard to overstate what other circumstances present graver risks of danger to human life than unilaterally deciding to transmit information related to plans for

kinetic military action between two countries. A significant sentence of imprisonment would complete the deterrent approach necessary to maximize the impact of this case as it relates to stopping others from committing the same brazen acts as the defendant.

In sum, the Court should balance the defendant's extremely dangerous conduct (warranting an upward variance from the applicable Guidelines range) with his swift actions (warranting mitigation) to resolve the case in determining a just sentence. Because his conduct would normally warrant a statutory maximum sentence of 120 months, a final sentence of 108 months' imprisonment does just that.

5. Avoid Unwarranted Sentencing Disparities

The Government's recommended sentence appropriately measures the defendant's culpability considering cases under the Espionage Act.

The defendant's case is analogous to that of defendant Jack Teixeira. Former U.S. Air National Guardsman Jack Teixeira was recently sentenced to 180 months' imprisonment after pleading guilty to retaining and disclosing on public websites hundreds of pages of national defense information, classified up to the Top Secret/SCI level. To be sure, the defendant's conduct differs in volume here, but his conduct was much more significant in the magnitude of potential harm and sensitivity of the materials he unlawfully disclosed, as detailed further in the classified supplemental memorandum. Teixeira was charged in connection with his theft and dissemination of classified information on Discord. As was the case here, once transmitted to Discord, the information eventually made its way across the Internet, potentially to some of America's adversaries. Like the defendant, Teixeira was a young man at the time of his crimes. Like the defendant, Teixeira had signed multiple non-disclosure agreements, had taken multiple trainings, and knew that his conduct was unlawful. And like the defendant, Teixeira's disregarded those

trainings and unlawfully transmitted classified information eventually published on the Internet. Like Teixeira's sentence, the defendant's sentence should reflect the seriousness of his crime.

Another recent prosecution under Section 793 that weighs in favor of a significant, above-Guideline sentence is *United States v. Schultz*, 3:24-CR-00056 (M.D. Tn. 2025). Korbein Schultz was a U.S. Army intelligence analyst who conspired with an individual he knew to be residing in Hong Kong to gather and transmit national defense information. Schultz ultimately provided his co-conspirator with dozens of sensitive documents, including documents related to China and its military, technical, and operational information about American weapons systems, U.S. military assessments of the Chinese military, U.S. military deployments, and how lessons from the Ukraine/Russia war could be applied to the defense of Taiwan. Although Schultz conspired with his Chinese handler to gather and transmit classified information, the Government did not have *any* evidence that Schultz successfully transmitted classified documents to his co-conspirator. Schultz pled guilty to, *inter alia*, conspiracy to gather and transmit national defense information, in violation of 18 U.S.C. § 793(g). The Government requested that Shultz serve 135 months in prison, and the Court ultimately sentenced Schultz to 84 months.

Like Schultz, the defendant in this case unlawfully disclosed sensitive military information. Like Schultz, the defendant was trained in the craft of intelligence and the importance of securing sensitive information and disregarded that training knowing full well that the disclosure of the information would be harmful to the United States. Unlike Schultz however, the defendant in this case *actually disclosed* classified, exceptionally sensitive information. Although Schultz's disclosures were undeniably harmful to national security, as the classified supplemental memorandum shows, the defendant's disclosures in this case were an order of magnitude more serious.

Additionally, the nature of the defendant's conduct is more serious than many other cases that are prosecuted under 18 U.S.C. §793(e), where individuals retain, but do not transmit, national defense information. For example, in *United States v. Edward McLean*, 3:22-cr-00115-TJC (M.D. Fl.), authorities found a flash drive in McLean's residence that contained approximately 150 documents containing Secret NDI, and 50 documents containing Confidential NDI. McLean received the statutory maximum sentence under 18 U.S.C. § 793(e)—120 months—for his retention of these documents.¹¹ Similarly, in *United States v. Christopher Glenn*, 9:14-cr-80031-KAM (S.D. Fla.) the court imposed the statutory maximum sentence of 120 months pursuant to 18 U.S.C. § 793(e), where the defendant pleaded guilty to removing Secret NDI from a Department of Defense network and storing those documents on removable media in his home.¹² Finally, in *United States v. Harold Martin*, 17-cr-00069-MJG (D. Md), a former contractor with the NSA was charged with unlawfully retaining a large amount of Top Secret information and sentenced to 108 months' imprisonment.

The scope of the defendant's conduct also distinguishes him from other individuals prosecuted under Section 793 that both retained and transmitted national defense information. For example, in *United States v. Reality Winner*, 17-cr-034 (JRH) (S.D. Ga.) the defendant printed and mailed to a media outlet a single intelligence report. Winner was sentenced to 63 months imprisonment. Here, as discussed above and in the Government's classified submission, the defendant's conduct far exceeds a single intelligence report.

¹¹ McLean was also sentenced to 160 months for distributing child sexual abuse material. His sentences are running concurrently.

¹² Glenn was subsequently sentenced to life in prison after a federal jury convicted him of sexually exploiting and trafficking in minors while working overseas.

Functionally, the consequences of the defendant's actions are much more akin to 18 U.S.C. § 794, which prohibits the delivery of NDI to a foreign government with the specific intent to harm the United States or aid a foreign power or reason to believe it would do so. For example, in *United States v. Jareh Dalke*, 22-cr-313 (D. Co.), a former NSA employee attempted to provide Top Secret information to an individual he believed was a Russian agent. Dalke was sentenced to 262 months' imprisonment. As detailed in the classified supplemental memorandum, the scope and magnitude of the defendant's conduct and the harm the defendant potentially caused is comparable to the harms caused by those who violate Section 794. When the defendant repeatedly sent NDI to numerous other individuals throughout 2024, the defendant knowingly exposed U.S. secrets in a manner that he knew could—and did—proliferate. And through his actions, the defendant ultimately provided Top Secret NDI to our allies and adversaries across the world via the internet. Seen against the backdrop of other prosecutions under the Espionage Act, the Government's recommendation is balanced in light of the defendant's conduct and would not create an unwarranted sentencing disparity.

CERTIFICATE OF SERVICE

I certify that on May 6, 2025, I filed electronically the foregoing with the Clerk of Court using the CM/ECF system, which will serve all counsel of record.

_____/s/
Troy A. Edwards, Jr.
Assistant United States Attorney
United States Attorney's Office for
the Eastern District of Virginia